(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2001 (10.05.2001)

PCT

(10) International Publication Number
WO 01/33317 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP00/10285

(22) International Filing Date: 18 October 2000 (18.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/162,503 29 October 1999 (29.10.1999) US
09/636,724 11 August 2000 (11.08.2000) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: EPSTEIN, Michael, A.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). STARING, Antonius, A., M.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: GROENENDAAL, Antonius, W., M.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

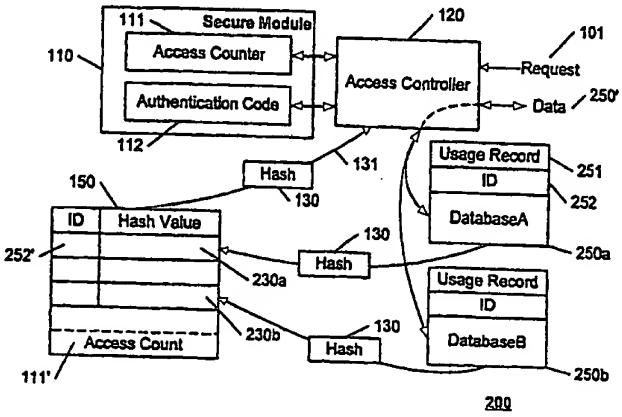
(81) Designated States *(national)*: JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ASSURING DATA INTEGRITY VIA A SECURE COUNTER



(57) Abstract: An access-control system includes a counter, and a secure memory location that is configured to contain a parameter that binds the contents of the counter to the data that is being protected. Each time the data is accessed, the counter is incremented and the binding parameter is updated, based on this new count. When a subsequent access is requested, the stored binding parameter is compared to a value corresponding to the binding of the current value of the counter with the data. If either the current value of the counter differs from the count that was used to produce the binding parameter, or the current data differs from the data that was used to produce the binding parameter, the new binding value will not correspond to the stored binding parameter, and access is denied. In this manner, a sequential access to the protected data can be enforced, thereby precluding a replay attack. Note that the data being protected may be data that is used to control access to other protected material, thereby expanding the scope of security protection to this other protected material.

WO 01/33317 A1

Assuring data integrity via a secure counter

This invention relates to the field of data security, and in particular to means for determining the integrity of data that changes with time.

A number of applications exist that depend upon maintaining control of the usage of data. In conventional data processing applications, it is often necessary to assure that the data being used is the most recent data. In secure applications, it is often necessary to assure that the data has not been tampered with.

In addition to a need for assuring that the data being used is current and valid, some data may have limits imposed for the number of times the data may be accessed, or the number of days that the data may be accessed. For example, a "try-before-you-buy" software application will typically control the number of times the application can be used. In like manner, a video playback system may be configured to control the number of times a recorded program is accessed, based on a purchased limited use license. To effect such a system, a usage parameter must be maintained. If this usage parameter is merely stored at a memory location, the access security system can be overcome by merely writing a new value to the memory location as required. A more sophisticated system may embed the usage parameter into an item that is bound to the limited-access material in a secure manner. For example, European patent EP0906700, "Method and system for transferring content information and supplemental information related thereto", issued 7 April 1999 to Johan P.M.G. Linnartz et al, presents a technique for the protection of copyright material via the use of a watermark "ticket" that controls the number of times the protected material may be rendered, and is incorporated by reference herein.

A common technique for overcoming a limited-access security systems is a "replay attack", wherein a copy of the usage parameter is recorded before its expiration is expired, and this recording is used to replay, or re-access, the material beyond the authorized access limits. In the case wherein the usage parameter is bound to the data being protected, such as via a watermark-based security system, the content material and all bound parameters

are recorded, for subsequent replacement, or "replay", as an authorized version of the material.

In like manner, a financial database may contain internal checks that facilitate a determination of counterfeit entries. A replay attack can be affected by obtaining a copy of a valid entry, such as a record or set of records showing a large balance in an account, then repeatedly substituting this record or set of records after withdrawing funds from the account.

It is an object of this invention to provide a security system that is not susceptible to replay attacks. It is a further object of this invention to provide a security system that verifies that the accessed data is the latest authorized version of the protected data.

This object and others are achieved by providing a system that includes a secure means of storing a usage parameter that is associated with each usage of the database, and a binding parameter that binds the usage parameter to the data that is being protected. Each time the data is accessed, the usage parameter is incremented and the binding parameter is updated, based on this new usage parameter. When a subsequent access is requested, the stored binding parameter is compared to a value corresponding to the binding of the current value of the usage parameter with the data. If either the current value of the usage parameter differs from the usage parameter that was used to produce the binding parameter, or the current data differs from the data that was used to produce the binding parameter, the new binding value will not correspond to the stored binding parameter, and access is denied. In a preferred embodiment, the usage parameter is a value that is contained in a sequential counter. In this manner, a sequential access to the protected data can be enforced, thereby precluding a replay attack. Note that the data being protected may be data that is used to control access to other protected material, thereby expanding the scope of security protection to this other protected material.

The invention is explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

Fig. 1 illustrates an example block diagram of an access-control security system in accordance with this invention.

Fig. 2 illustrates an example block diagram of an alternative access-control security system in accordance with this invention.

Fig. 3 illustrates an example flow diagram for an access-control security system in accordance with this invention.

Throughout the drawings, the same reference numerals indicate similar or corresponding features or functions.

Fig. 1 illustrates an example block diagram of an access-control security system 100 that controls access to the contents of a database 150. An access controller 120 receives an access request 101, and grants the request only if the database 150 is authenticated as being current. A secure module 110 contains a counter 111 that maintains a usage parameter 111' that is incremented with each access to the controlled database 150. In accordance with this invention, this usage parameter 111' is bound to the database 150, preferably by computing a hash value 131 corresponding to the data base 150 and the usage parameter 111', via a hash generator 130. A counter 111 is presented herein as a paradigm for a device that provides a substantially unique value with each access to the database. Alternatively, a random number generator or other 'unique value generator' can be used in lieu of the counter 111 to uniquely identify each access to the database 150. By using a counter 111, the number of times that the protected database 150 is access can also be determined, and usage-limiting rules can be enforced, as discussed further below.

As is common in the art, the hash generator 130 provides a one-way computation of a hash value based on a set of input values, such that knowledge of the hash value provides no information regarding the value of any of the set of input values. Most significantly, it is computationally infeasible to determine a set of input values that will produce a specified hash value 131. A change of any item in the database 150 or the usage parameter 111' data item will produce a different hash value 131. That is, each access to the database 150 in accordance with this invention generates a unique hash value 131 whose value depends upon the usage parameter 111' and the contents of the data base 150.

In some applications, the contents of the database is fixed; for example, a CD or DVD recording of entertainment material. In other applications, the database is modifiable. If the database can be modified, a preferred embodiment of this invention uses the database to store the usage parameter 111', thereby eliminating the need to provide an access counter 111 in the secure module 110. Storing the usage parameter 111' in the

database 150 also eases the hash generation task at 130, because hash routines are commonly available that compute a hash value corresponding to a data file. The access count device 111 is illustrated in the figures as being contained in the secure module 110, as the more general solution (independent of whether the database 150 is modifiable). Additionally, the usage parameter 111' is illustrated as being associated with the database 150, via the dashed block, indicating that the usage parameter 111' is used in computing the hash 131, regardless of whether the usage parameter 111' is stored in the database 150 directly, or in an access count device 111 within the secure module 110.

The unique hash value 131, or a parameter based on this unique hash value 131 is stored in the secure module, as an authentication code 112. Upon each access to the database, the usage parameter 111' is changed, a new hash value 131 is computed, and a new authentication code 112 is stored, replacing the prior authentication code. When a subsequent access request 101 is received, a hash 131 of the current database 150 and usage parameter 111' is computed, and compared to the stored authentication code 112. If the usage parameter 111' is not included within the database 150, the current value of the access counter 111 is used to compute the new hash value 131. If another database has been substituted for the latest version of the database, such as a prior version of the database, with an earlier usage parameter, the hash 131 of this substitute database will not match the stored authentication code 112, and access is denied. If the current database 150 is the latest version of the database, the hash 131 will match the stored authentication code 112, and access will be granted.

Note that, as thus far presented, this invention provides a secure system and method for determining whether a current copy of a database corresponds to the latest version of a database. In addition to preventing successful replay attacks, this invention also protects against unauthorized modifications to the database. Conventional security techniques may be included in the access control 120 to assure that only authorized users are permitted to modify the database, including the use of passwords, cryptographic keys, access cards, smart cards, and the like. If the database is modified by a system other than one with access to the secure module 110, a new authentication code 112 will not be generated for this modified database, and therefore an attempt to substitute this modified database for the latest authorized database will fail. In a financial database system, for example, each transaction is gated by an access controller 120 having access to the secure module 110; any substituted records in the database 150 will result in an access denial, as discussed above.

Additional access controls may also be employed. If the database 150 has a limit to the number of times it may be accessed, corresponding, for example, to a limited use license, the usage parameter 111' is used to determine whether the number of accesses is within the limit. If the usage parameter 111' indicates that the limit has been reached, access is denied.

Fig. 2 illustrates an example block diagram of an alternative access-control security system 200 in accordance with this invention. In system 100 of Fig. 1, it is assumed that the usage parameter 111' is bound directly to the contents of the database 150. In system 200 of Fig. 2, the usage parameter 111' is bound indirectly to the contents of a plurality of databases 250a, 250b. A hash value 230a, 230b is computed and stored in the database 150 for each of the plurality of databases 250a, 250b. A hash value 131 is computed based on the contents of the database 150 and the usage parameter 111', and stored as the authentication code 112, as discussed above. The access controller 120 authenticates each dataset 250a, 250b by comparing a hash of its contents to the stored value in the current database 150, and authenticates the current database 150 by comparing its hash value 131 to the stored authentication code 112.

If any of the databases 250a, 250b have a limit to the number of times they may be accessed, a usage record 251 is included within the corresponding database 250a, 250b, and the value of this usage record 251 is thereby included in the determination of the hash value 230a, 230b that is stored in the database 150. Other items that facilitate organization and control, such as a unique ID 252 for each database 250a, 250b, are also included.

Fig. 3 illustrates an example flow diagram for an access-control security system in accordance with this invention. At 310, an access request is received. A hash of the database and usage parameter is computed, at 320, and compared to an authentication code that is stored in a secure location, at 330. If, at 335, the hash does not correspond to the stored authentication code, access is denied, at 340. If, at 335, the hash corresponds to the stored authentication code, the usage parameter is incremented, at 350. As noted above, this usage parameter may be stored in the associated database, or in the secure location that contains the authentication code, at 360. After incrementing, or otherwise modifying, the usage parameter, access to the database is granted, at 370. At the completion of access to the database, a hash of the database, with the usage parameter, is computed, at 380, and stored as the new authentication code in the secure location, at 390. Alternative flows will be evident to one of ordinary art. For example, in the illustrated flow of Fig. 3, a discontinuity of flow 360-390

will result in a stored usage parameter that does not correspond to the stored authentication code. Techniques common in the art can be used to assure a synchronization between the usage parameter and authentication code is maintained. For example, each time the usage parameter or database is changed, a corresponding authentication code can be generated and stored in a temporary location, and a recovery routine can be provided to recover the latest versions of the database, usage parameter, and authentication code in the event of a discontinuity of flow in the sequence of Fig. 3.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within its spirit and scope. For example, the specific physical embodiment of this invention may take a variety of forms. A solid-state memory module with smart card functionality may comprise the secure module 110. The secure module 110 may be embodied as an encoding that only 'compliant devices' are able to read or write, a compliant device being one that is manufactured by manufacturers who agree to abide by certain rules and standards established for protecting recorded material. The encoding may include the use of cryptographic keys that are secret to the complying manufacturers, or may include the use of special purpose hardware devices for reading and writing the secured information. The secure module, the database, and the access controller may each be embodied as discrete components. For example, the secure module may be a smart card, the database may be a file on a remote computer, or at a site on the Internet, and the access controller may be an embedded program in a processor of a playback device. As noted above, the security of the secure module may be provided via the use of encryption keys and the like, and therefore the entire system can be embodied as a software application. These and other system configuration and optimization features will be evident to one of ordinary skill in the art in view of this disclosure, and are included within the scope of the following claims.

CLAIMS:

1. A security system (100, 200) comprising:

an access device (120) that is configured to control access to protected data (150),

a first memory (111) that is configured to contain a usage parameter that is modified by the access device (120) when the protected data (150) is accessed,

a secure module (110), operably coupled to the access device (120), that includes:

a second memory (112) that is configured to contain an authentication code that is based on the protected data (150) and the usage parameter when the protected data (150) is accessed.

2. The security system (100, 200) of claim 1, wherein

the access device (120) is further configured to control access to the protected data (150) based on a usage limit, the usage parameter, and the authentication code.

3. The security system (100, 200) of claim 1, further including

a hash generator (130) that is configured to generate a hash value corresponding to the authentication code that is dependent upon the protected data (150) and the usage parameter.

4. The security system (100, 200) of claim 1, wherein

the protected data (150) includes a plurality of parameters (230), each parameter corresponding to one of a plurality of other protected data (250).

5. The security system (100, 200) of claim 4, wherein

each parameter (230) corresponds to a hash value that is dependent upon the corresponding one of the plurality of other protected data (250).

6. The security system (100, 200) of claim 5, wherein

the authentication code corresponds to an other hash value (131) that is dependent upon the protected data (150) and the usage parameter.

7. The security system (100, 200) of claim 1, wherein
the secure module (110) corresponds to at least one of:
a smart card, and
an encoding in a secure format.

8. The security system (100, 200) of claim 1, wherein
the first memory (111) is included in one of:
a storage media that includes the protected data (150), and
the secure module (110).

9. The security system (100, 200) of claim 1, wherein
the first memory (111) corresponds to a memory of a counter, and
the access device (120) modifies the first memory (111) by incrementing the counter.

10. A method of controlling access to protected data (150), comprising:
computing (320) a hash value based on the protected data (150) and a usage parameter,
comparing (330) the hash value to an authentication code that is stored in a secure location, and
denying access (340) to the protected data (150) based on the comparison of the hash value and the authentication code.

11. The method of claim 10, further including:
modifying (350) the usage parameter,
computing (370) a second hash value based on the protected data (150) and the modified usage parameter, and
storing (380) the second hash value as the authentication code in the secure location.

12. The method of claim 11, further including:

storing (360) the usage parameter with the protected data (150).

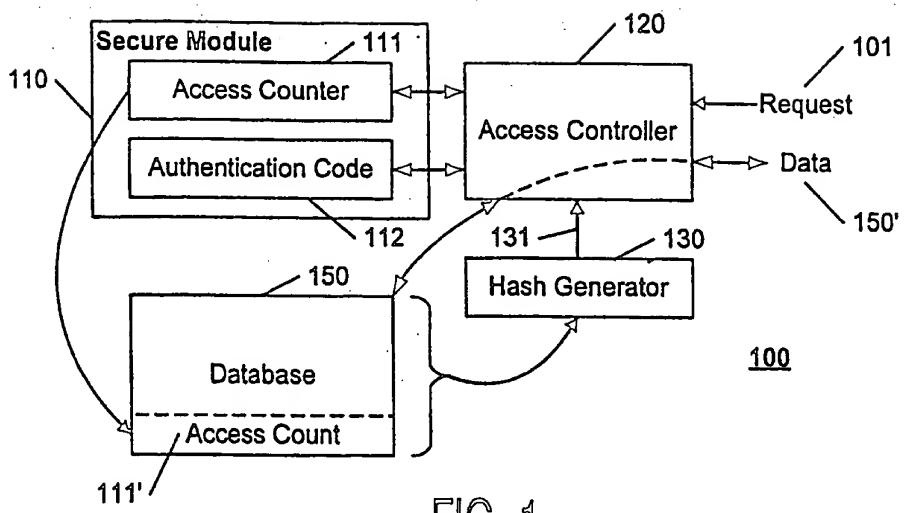

Secure Module
111
110
Access Counter
Authentication Code
112
120
Access Controller
101
Request
Data
150'
131
130
Hash Generator
150
Database
Access Count
111'
100

FIG. 1

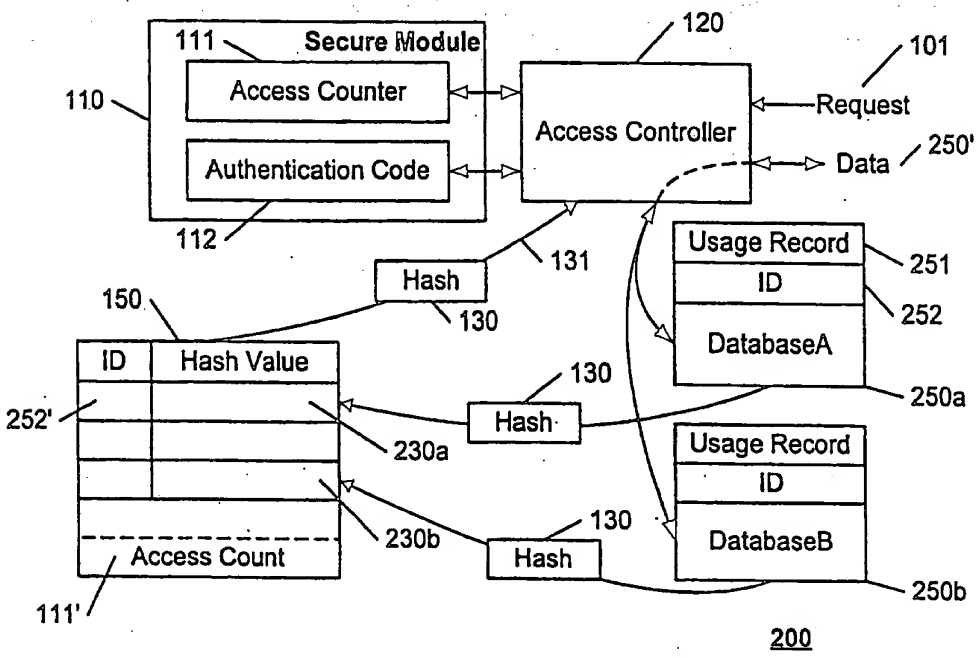

111
Secure Module
110
Access Counter
Authentication Code
112
120
Access Controller
101
Request
Data
250'
131
Hash
130
150
ID
Hash Value
252'
230a
230b
Access Count
111'
Usage Record
ID
DatabaseA
251
252
250a
Hash
130
Usage Record
ID
DatabaseB
Hash
130
250b
200

FIG. 2

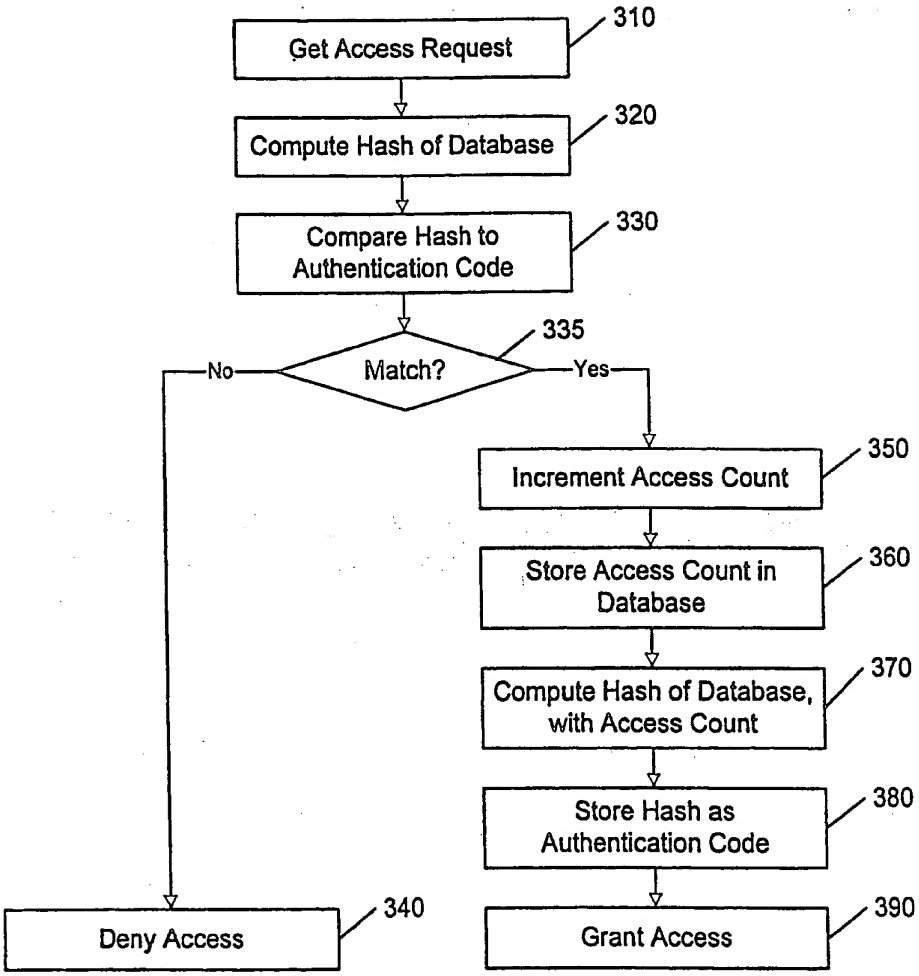

Get Access Request
310
Compute Hash of Database
320
Compare Hash to Authentication Code
330
Match?
335
No
Yes
Increment Access Count
350
Store Access Count in Database
360
Compute Hash of Database, with Access Count
370
Store Hash as Authentication Code
380
Deny Access
340
Grant Access
390

FIG. 3

INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/EP 00/10285

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 881 561 A (HEWLETT PACKARD CO) 2 December 1998 (1998-12-02) column 1, line 1 - line 9 column 2, line 26 -column 3, line 12	1,2,7-9
Y	column 7, line 38 - line 50 column 9, line 52 -column 10, line 36	3-6, 10-12
Y	EP 0 845 733 A (SUN MICROSYSTEMS INC) 3 June 1998 (1998-06-03) column 7, line 17 -column 8, line 37 column 9, line 6 - line 23; figures 3A,3B	3-6, 10-12
A	US 4 658 093 A (HELLMAN MARTIN E) 14 April 1987 (1987-04-14) column 5, line 57 -column 6, line 2 column 6, line 16 -column 7, line 16 column 11, line 4 - line 19	1,3,7,10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 January 2001	05/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, L

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr ıal Application No
PCT/EP 00/10285

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0881561 A	02-12-1998	US 5327563 A	05-07-1994
		DE 69326119 D	30-09-1999
		DE 69326119 T	20-01-2000
		EP 0598587 A	25-05-1994
		US 5628015 A	06-05-1997
EP 0845733 A	03-06-1998	US 6021491 A	01-02-2000
		US 5958051 A	28-09-1999
		JP 10326078 A	08-12-1998
US 4658093 A	14-04-1987	NONE	